Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Justice and Police FDJP
Post and Telecommunications Surveillane Service PTSS

Annual Report 2024
PTSS

Telecommunications surveillance must be viewed in its global context. English is the standard language used at international conferences, in international bodies and in the telecommunications industry itself. The English term Lawful Interception (LI) is now also widely used here in Switzerland. The Post and Telecommunications Surveillance Service adopted the use of the standard terminology in 2010. Since then, it has had its own website, at:

www.li.admin.ch

Dear reader

I was delighted to begin my new role as head of the PTSS in February 2024, but also acutely aware of the responsibility I was taking on. The past few months have been full of comprehensive insights, new challenges and beneficial interactions with dedicated colleagues – not just within the PTSS, but also with the different cantons, federal authorities and entities obliged to cooperate (communications service providers). In an era of rapid technological transformation and changing legal frameworks, our aim is to future-proof the PTSS and carry out our tasks with the utmost professionalism and rigour. We have also incorporated these priorities into our newly developed strategy (see our new mission statement on p. 11). The importance of our role as a central hub in the field of telecommunications surveillance is particularly evident when it comes to ensuring data quality and keeping pace with new technologies. Our role enables us to ensure that legal and technical requirements are implemented efficiently and that there is smooth cooperation between all stakeholders. It also allows us to safeguard the interests of the state while protecting individuals' fundamental rights.

This annual report examines these and other key points. It also describes the challenges we have overcome and our achievements, showing how we have emerged from 2024 as a stronger organisation.

I would particularly like to highlight an important milestone for us and our partner organisations: after almost a decade of intensive work, the Telecommunications Surveillance Programme was completed successfully. It was a major challenge, but also an opportunity to develop innovative solutions and set new standards. Technological developments are advancing inexorably,

> "When it comes to ensuring data quality and keeping pace with new technologies, the importance of our role becomes clear."

increasing the demands on our system's integrity and performance. By switching from a monolithic system to modular, flexible components such as the Federal Lawful Interception Core Component (FLICC), we have laid the groundwork for keeping pace with these developments. Our new system structure allows us to respond quickly and precisely to technological changes and new requirements (see article on p. 17).

Telecommunications surveillance is a complex set of tools that requires careful coordination between our system and the networks operated by TSPs. To keep everything running smoothly, tests are required – such as the surveillance test drives we are carrying out together with the Zurich Cantonal Police. This initiative is also an excellent example of the close and trusting cooperation we enjoy with our national and international partners. Through mutual exchange, we can respond proactively to developments and work together to find solutions (see article on p. 25).

But we don't just want to develop our system components – it goes without saying that we want our employees and customers to be able to develop, too. With this in mind, the PTSS offers classroom-based and online training courses tailored to users' varying levels of knowledge, from beginners through to specialists, helping them to work in a constantly evolving technological environment. The Incident Management Team also provides essential technical support and ensures that any problems reported by users are resolved quickly (see article on p. 22).

Our combination of technical excellence, transparency and efficient cooperation with our customers and partners creates added value for law enforcement in Switzerland. This is only possible thanks to the dedication of everyone involved: from our internal teams and external partners to the law enforcement agencies and organisations that are obliged to cooperate with us.

The completion of the Telecommunications Surveillance Programme marks the dawn of a new era – one in which we will not only build on our achievements, but also explore new avenues. Let's take this journey together, with an innovative spirit, dedication and close cooperation.

I hope you enjoy reading this report!

Daniela Schär
Head of the PTSS

01

OVERVIEW

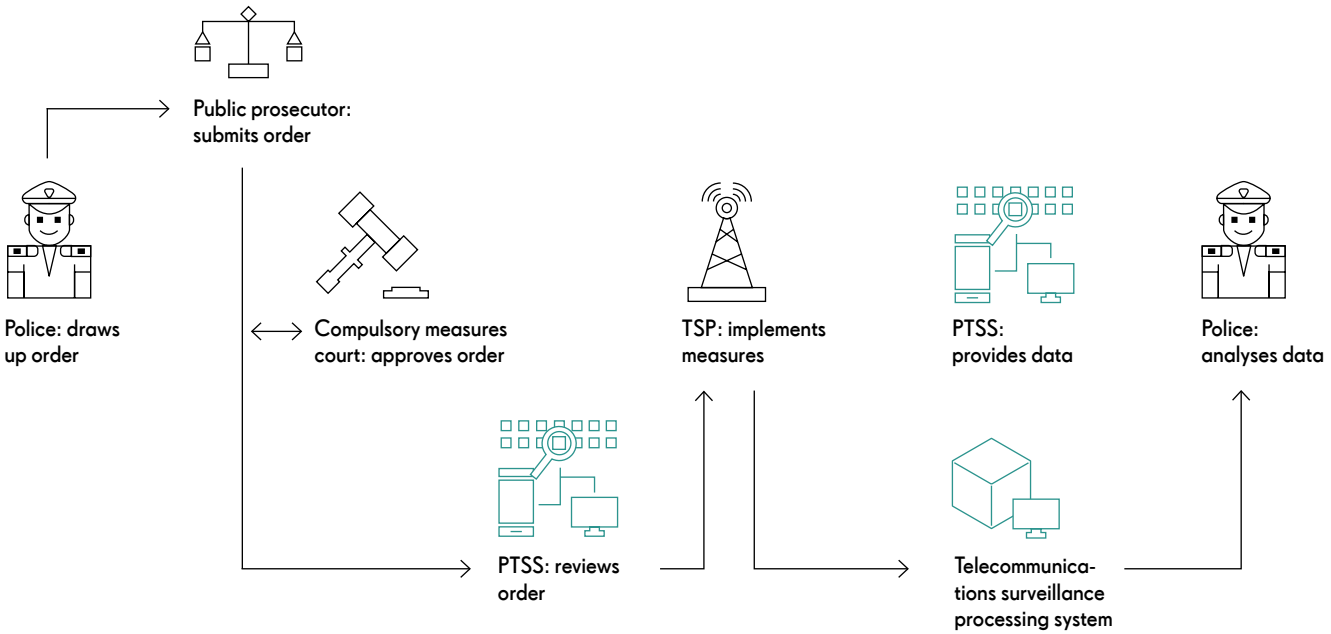
The PTSS: an overview

When investigating serious offences, the federal and cantonal law enforcement authorities can order measures to conduct surveillance of postal and telecommunications activity. Since 1 September 2017, the Federal Intelligence Service (FIS) has also been authorised to order surveillance measures from the Post and Telecommunications Surveillance Service (PTSS) in case of a threat to Switzerland's internal or external security. Since 1 January 1998, the PTSS has been responsible for carrying out these measures and ensuring they comply with legislation and the rule of law. The law enforcement authorities make a request for data to the PTSS, which obtains the data from the telecommunications service providers (TSPs); this is then passed on to investigators for analysis. The PTSS also ensures that the applicable legislation is observed and that the public's fundamental right to privacy is protected. The PTSS acts independently and autonomously and is not subject to directives from other authorities. It is affiliated for administrative purposes to the IT Service Centre of the Federal Department of Justice and Police (ISC-FDJP).

Neither crime nor modern telecommunications recognise territorial borders, so international cooperation plays an essential role in the fight against crime. The PTSS works to promote international standardisation and the exchange of knowledge and information with our counterparts abroad.

The PTSS is organised into three divisions, each of which is divided into three teams.

The surveillance process



The PTSS management team (from left to right): Jean-Louis Biberstein, Daniela Schär, Michael Galliker, Alexandre Suter

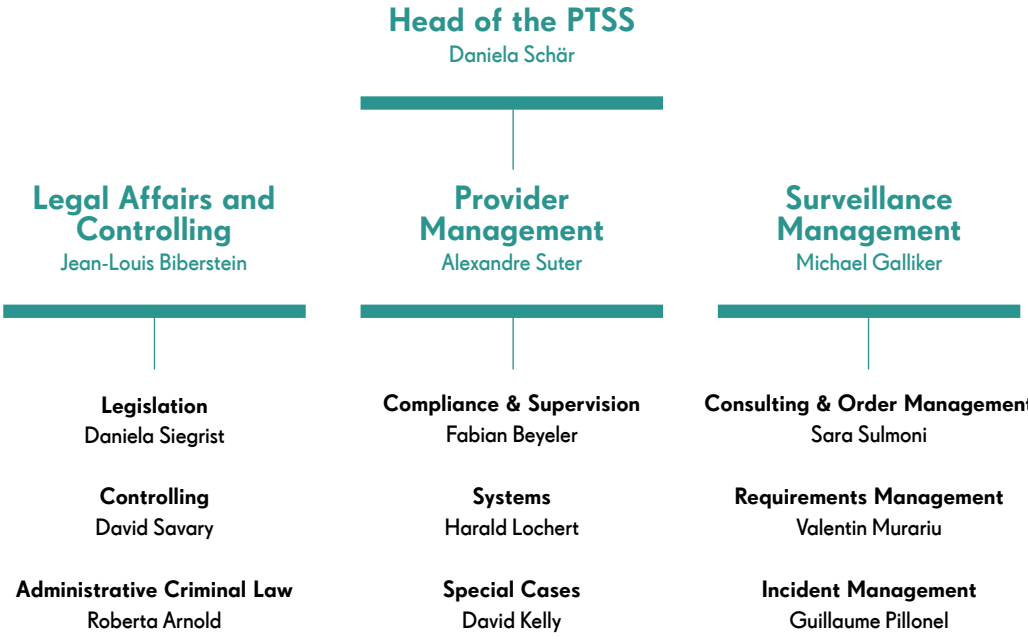
Legal Affairs and Controlling

The **Legal Affairs and Controlling Division** is responsible for the legal and operational framework of the PTSS's work. The team is tasked with drawing up the necessary legal framework to ensure that telecommunications surveillance is conducted correctly. This safeguards the public's right to privacy and is a key requirement in ensuring that the data gathered can be used in court. The Legal Affairs and Controlling Division is split into three teams: Legislation, Controlling and Administrative Criminal Proceedings.

The **Legislation Team** is responsible for the entire legislative process at the PTSS. This includes implementing primary and secondary legislation projects related to postal and telecommunications surveillance. For example, the FDJP Ordinance on the Implementation of Post and Telecommunications Surveillance (OI-PTS) is reviewed periodically and amended if necessary. In many cases, this involves adapting ordinances to reflect the latest technological changes. This team also represents Switzerland and participates in national and international standardisation bodies, handles political affairs in collaboration with the General Secretariat and administers training. In addition, it provides in-house advice and support in all proceedings involving the administration of justice. Staff respond to media enquiries and handle requests for information from the public.

The **Controlling Team** performs cross-cutting functions for the PTSS, including financial management, controlling and reporting. It issues invoices to law enforcement authorities and the FIS and makes compensation payments to TSPs. Legal project support and risk and process management also fall within the team's remit. The organisational unit's IT security officer and data protection officer are members of this team.

The **Administrative Criminal Proceedings Team** exercises the PTSS's administrative criminal law competences and conducts proceedings on its behalf. In so doing, it acts independently and is not subject to directives.



Provider Management

The **Provider Management Division** is responsible for all matters relating to cooperation between the PTSS and persons and entities obliged to cooperate with it. The division has supervisory authority over the latter and responsibility for the processing system, including all PTSS applications. The staff also manage relationships with more than 1,000 providers, advise them on technical and legal matters, and issue related orders and decisions within the scope of their supervisory authority. In addition, the division shares information and knowledge with other departments in Switzerland and abroad. The Provider Management Division is split into three teams: Compliance and Supervision, Special Cases and Systems.

The **Compliance and Supervision Team** is responsible for maintaining relations with persons and entities obliged to cooperate with the PTSS. This includes advising them on legal, technical, organisational and administrative matters. Under the SPTA, TSPs must at all times be able to conduct surveillance of the services they offer and to provide the associated data and information, unless they have been duly exempted from the obligation to do so. The Compliance and Supervision Team verifies this willingness to carry out surveillance and provide information (known as the compliance procedure). The team also exercises the PTSS's supervisory authority over those required to cooperate with it.

For TSPs that are not themselves able or legally required to do so, the Provider Management Division develops and operates tailor-made solutions for implementing surveillance measures. These cases are handled by the **Special Cases Team**. It is involved when, for example, a small provider such as a local cable network operator or a hotel is required to conduct surveillance activities. This team is responsible for developing and operating all customised and complex surveillance measures.

The **Systems Team** ensures the smooth operation and continuing development of the appli-

cation landscape for the telecommunications surveillance processing system (PTSS processing system). The team implements clients' and specialist bodies' requirements and ensures that the components of the PTSS processing system are operated in accordance with the relevant specifications. Alongside the application manager, product owners are responsible for the applications throughout their entire life cycle, including planning, implementation, ongoing development and system expansion in productive operation. They maintain relationships with suppliers and service providers (see article on page 17).

Surveillance Management

The **Surveillance Management Division** handles the PTSS's interaction with law enforcement authorities and the FIS. It takes care of operational business, specifically order processing, consulting and incident management. Along with the IT Service Centre (ISC-FDJP), its staff are the single point of contact in case of problems with the processing system or other difficulties experienced by users. This division is also involved in the development of new applications. The Surveillance Management Division is split into three teams: Consulting and Order Management, Requirements Management and Incident Management.

The **Consulting and Order Management Team** advises police forces, public prosecution services, compulsory measures courts and the FIS on legal, technical, organisational and administrative matters. It examines, processes and monitors surveillance orders, emergency searches and searches for wanted persons. Staff receive surveillance orders, which they subject to a formal check before passing them on to the TSPs. They then ensure that law enforcement authorities receive the data supplied by the TSPs. The team also processes requests for information.

The **Requirements Management Team** ensures that the telecommunications surveillance processing system is adapted to users' changing requirements. The division plans and manages all IT projects critical to the PTSS's mandate. It is also responsible for project management and architecture for brand-new initiatives.

The **Incident Management Team** deals with problems affecting data transmission in operational business. The team also provides technical advice in complex cases and organises information events and training courses for the relevant authorities.

Outside office hours, Surveillance Management provides standby cover with the technical support of the Provider Management Division in particular. As such, the PTSS is available around the clock.

The new mission statement

Last year, the PTSS revised its strategy. An interdisciplinary working group, consisting of representatives from all hierarchy levels and divisions, was formed to develop a forward-looking mission statement. The aim of this process was to create a long-term strategy that will strengthen the PTSS over the long term and ensure it is ideally prepared for future challenges.

The strategy was developed in several coordinated stages. Firstly, a comprehensive SWOT analysis was carried out to systematically identify strengths, weaknesses, opportunities and threats. Law enforcement agencies and TSPs were also involved in this process. The working group then drew up a mission statement and the underlying vision and mission. The next stage consisted of formulating the PTSS's values. All employees were involved to ensure broad acceptance of and identification with its strategic goals. These values were then used to formulate the strategic priorities that will determine the PTSS's future path. Looking ahead, the next stage will involve implementing the strategy consistently so that we can achieve our goals in the long term.

The PTSS's mission has three main elements: firstly, we make a significant contribution to investigating and combating crime. Secondly, we provide effective assistance in searching for and rescuing missing persons whose physical integrity or lives are at serious risk. And thirdly, we act as a crucial intermediary between law enforcement agencies and entities that are obliged to cooperate with us.

The PTSS's vision is based on a proactive approach and has a strong focus on innovation. Our range of services is optimised regularly thanks to targeted engagement with contacts in Switzerland and abroad. At all times, however, our main priorities are to comply with our legal framework and protect the data entrusted to us.

The vision described above forms the basis of our strategic direction. At the PTSS, we are focusing on technological sovereignty and operational efficiency to allow us to carry out our tasks with the utmost precision. We are also optimising stakeholder communication so that we can strengthen our dialogue with partners and stakeholders. One of our main focuses is forward-looking innovation, especially the use of new technologies. And finally, we must ensure compliance and security to guarantee our long-term success and sustainability.

This strategic realignment will enable us to engage with future challenges and create a solid foundation for an efficient and resilient organisation.

What is our purpose?

The PTSS ensures that postal and telecommunications traffic is monitored efficiently and effectively. It helps to prevent and investigate criminal activity, making an important contribution to Switzerland's internal security and protecting the general public's fundamental rights. During emergency search operations, the PTSS provides relevant information so that individuals in danger can be located quickly. The PTSS also serves as the interface between various law enforcement authorities and communications service providers.

Mission

Where do we want to go?

One step ahead – as a reliable partner for Switzerland's internal security.

Vision

How do we want to develop?

- Strengthen technological sovereignty and autonomy
- Increase operational efficiency
- Optimise stakeholder communication
- Expand forward-looking innovation capacity
- Ensure compliance and security

Strategic priorities

In everything we do, we…

embrace transparency.
We are honest and, when problems arise, we communicate the facts clearly, comprehensively and transparently.

act constructively.
We act constructively by giving feedback and delivering concrete results together.

work together.
We support each other by taking the time to help each other and make progress as a team.

Values

A look back at 2024

January

FO-SPT and first partial revision of SPTO (5G)
The new financing ordinance (FO-SPT) came into effect on 1 January. As a result, the cantons now have to pay their share of the costs only once a year (annual flat rates).

A lump sum is now also paid to entities obliged to cooperate with the PTSS. However, smaller providers are still compensated on a case-by-case basis.

Three revised implementing ordinances relating to the SPTA also came into force on 1 January. These were adapted to account for technological developments, including 5G technology. The aim was to avoid gaps in telecommunications surveillance, enable more precise positioning and continue ensuring effective law enforcement.

February

Head of the PTSS
There was change at the top of the PTSS on 1 February: Tobias Beljean, interim head of the PTSS since 1 June 2023, handed over the reins to Daniela Schär.

March

FLICC goes live
FLICC (Federal Lawful Interception Core Component), the new component of the telecommunications surveillance processing system for real-time surveillance, went live on 18 March. This means that all real-time surveillance are now provisioned in FLICC, not ISS.

April

Report in response to postulate 19.4031 by Albert Vitali
(For a proportionate Federal Act on the Surveillance of Post and Telecommunications)
The head of the PTSS was invited to speak about the postulate at the meeting of the National Council Transport and Telecommunications Committee (TTC-N) on 29 April.

May

Parliamentary question 24.1007 Pfister Gerhard
(Financing the surveillance of post and telecommunications. Federal government vs cantons)
On 22 May, the Federal Council answered a question from National Councillor Gerhard Pfister on the financing of telecommunications surveillance. In particular, the Federal Council commented on the commencement of the FO-SPT and the distribution of costs between federal government and the cantons.

June

ETSI meeting in Lucerne
The 66th plenary meeting of the European Telecommunications Standards Institute's Technical Committee Lawful Interception (ETSI TC LI) was held in Switzerland for the first time from 18 to 21 June. The event was organised and hosted by the PTSS. A total of 97 participants from 20 different countries attended and networked in person.

Farewell ISS!
The last surveillance measures that were still sending data to ISS were deactivated at the end of June. This meant that work could continue as planned in preparation for retiring the system at the end of the year.

Handover of Telecommunications Surveillance Programme to PTSS
On 30 June, the Telecommunications Surveillance Programme came to a close and the programme organisation structure was dissolved. In the runup to that day, all projects had been successfully completed and all applications and components had been handed over to the relevant parent organisations (the PTSS, fedpol, ISC-FDJP operational organisation) for operation and further development (see article on p. 17).

A broadly based organisation

The programme on developing and operating the telecommunications surveillance processing system and federal police information systems (Telecommunications Surveillance Programme) ended in mid-2024. Several new components in the telecommunications surveillance processing system, a national investigation system (NES) and GovWare have been introduced. The PTSS and fedpol are now responsible for completing any outstanding tasks from the various projects, for operating the systems and for further development. Following the programme's completion, the established programme and project structures – and therefore some committees – were dissolved. The remaining committees will be streamlined on the basis of a recommendation from the project 'Zukunft Erhebung und Auswertung von Kommunikationsdaten zur operativen Ermittlungsunterstützung in der Schweiz' (Future collection and evaluation of communication data for operational investigation support in Switzerland, commonly referred to as ZEAKES).
The end of the Telecommunications Surveillance Programme and the reorganisation of the Criminal Investigation IT and Technology specialist unit present an opportunity to implement the ZEAKES recommendations by creating a broad-based organisation within the public administration. This organisation would involve a wide range of institutions and would provide a comprehensive overview, coordination and cooperation at national level. Its portfolio would cover not only telecommunications surveillance issues, but also issues related to criminal investigation technology in general. This would enable processes for decision-making, coordination, innovation and harmonisation to be put in place.
The proposed organisation would involve institutions at all federal levels in political, strategic, organisational and tactical matters, with project management tasks across all these areas.
Discussions about setting up this organisation have already taken place at various levels.
A pilot of the new committee landscape will be launched at the start of 2025. The performance of the new committees will be evaluated in autumn 2025, with the definitive launch following approval by the autumn meeting of the CCJPD and the General Secretariat of the FDJP. After the launch, the committee landscape will be evaluated on a regular basis and modified if necessary.

July

Draft treaty with the Principality of Liechtenstein
A treaty on telecommunications surveillance cooperation between Switzerland and the Principality of Liechtenstein was drafted to replace the exchange of notes from 2003. Working with the Federal Office of Justice, the PTSS finalised the zero draft of the treaty and delivered it to Liechtenstein's negotiating partners on 12 July.

August

2nd revision of STPO (scope of application)
On 5 August, the draft for the second revision of the Ordinance on the Surveillance of Post and Telecommunications (SPTO) was submitted for official consultation. The consultation process ran until 23 August. The input received from the various federal administrative units was then reviewed and consolidated.

September

Revision of the telecommunications surveillance committee landscape
One of the recommendations from the ZEAKES project launched in 2020 was to streamline the committee landscape. A meeting to discuss this issue was held on 30 September. The amended version of the committee landscape was discussed, and the further procedure for consulting with current and future representatives was established (see information box).

October

New Annex 1 to OI-PTS in force
The latest revision of Annex 1 to the FDJP Ordinance on the Implementation of Post and Telecommunications Surveillance (OI-PTS) came into force on 1 October. As such, the technical regulations on the interfaces for telecommunications surveillance have been adapted to meet ETSI's new international standards.

November

LI Day 2024
After a gap of five years, another Lawful Interception Day (LI Day) was held at the National Hotel in Bern on 19 November. The numerous presentations on issues relating to the PTSS were very well received by the participants. As usual, the event was also a welcome opportunity for networking and discussion.

Switzerland – Liechtenstein treaty
On 27 November, a Swiss delegation made up of PTSS and FOJ representatives travelled to Vaduz to open negotiations on the treaty with the Principality of Liechtenstein.

December

2024 customer satisfaction survey
Every two years, the PTSS conducts a customer satisfaction survey. This year's survey showed that satisfaction continued to rise. On a scale from 1 (very dissatisfied) to 6 (very satisfied), the following scores were achieved:

- Overall satisfaction of evaluating authorities: Improvement from 4.9 to 5.1
- Overall satisfaction of ordering authorities: Improvement from 4.9 to 5.0
- Overall satisfaction of approving authorities: Improvement from 5.5 to 5.7

FLICC was very well received compared to the component it replaced. As a result, satisfaction with the user-friendliness and comprehensibility of real-time surveillance data increased significantly – by 0.7 and 0.4 points respectively.

02

BACKGROUND

Telecommunications Surveillance Programme

The dawn of a new era

The world is changing rapidly, and things that are in fashion now will soon be old news. But criminals are equally quick to find ways to exploit the latest technologies for their own gain. The PTSS has taken action to keep pace with this reality.

At the Federal Council's request, Parliament adopted the Telecommunications Surveillance Programme in 2015 to make Switzerland better equipped for the challenges of rapid technological change.

The programme ran in several stages. At the end of 2024, the previous real-time surveillance system ISS (Interception System Switzerland) was switched off after being phased out and fully replaced by new components. "ISS was designed for the state of the art at the time," says Harald Lochert, head of the Systems Team at the PTSS, "and it was like an oil tanker: powerful, but slow to change course. We have now replaced ISS with a fleet of nimble speedboats that can be steered quickly whenever we need to change direction."

Let's go back to the beginning. In 2014, the Federal Council requested a guarantee credit of CHF 99 million from Parliament for a new programme to expand and upgrade the PTSS's surveillance systems and the Federal Office of Police's (fedpol) information systems. At that time, ISS was not yet in operation, and the public debate was influenced by the NSA wiretapping scandal revealed by Edward Snowden. And yet everyone agreed that the system needed to be expanded in the future. Technical developments were advancing rapidly, and the PTSS had to ensure that it could fulfil its legal obligations in the long term. In addition, the information and order management systems had both reached the end of their life cycles.

And so, after several years of planning, the programme began. It ran for almost ten years before being brought to an end in summer 2024. A programme organisation team was set up, consisting of the PTSS, fedpol, the IT Service Centre

Team leader Harald Lochert (right) with his product owners Arie Band (left) and Christoph Nickel (centre)

"We have replaced the sluggish tanker with a fleet of nimble speedboats."

Harald Lochert, Team Leader systems

(ISC-FDJP) and external consultants and suppliers. The first stage in early 2019 was to replace the components that had reached the end of their service life. The new information system IRC (Information Request Component) enables the PTSS to facilitate information sharing between telecommunications providers and law enforcement agencies. For example, if law enforcement agencies want to know the name under which a particular telephone number is registered, they request this information via IRC. The order management system WMC (Warrant Management Component) in turn allows digital logging of all surveillance orders. This full digitalisation of processes later proved invaluable during the coronavirus pandemic.

The RDC (Retained Data Component) was added in November 2020. This is used to send retrospective surveillance data and offers visualisation and grouping features. Finally, a pilot phase was launched in 2023 to replace ISS with FLICC (Federal Lawful Interception Core

Component), a real-time surveillance component. This has a modular structure, which means that the individual modules and functions are independent of each other and easy to replace, allowing for rapid development. Without this modularity, the entire system would have to be rebuilt if a technical standard were to change.

When introducing FLICC, it was also important to ensure independence from individual suppliers. The source code for the application belongs to the PTSS, which means that if any modifications are required, the PTSS can handle them itself. This guarantees flexibility, and user requests and suggested changes can also be implemented more quickly.

After the Telecommunications Surveillance Programme ended on 30 June, full responsibility for the newly introduced components was handed over to the PTSS. Four product teams are currently in charge of its operation and further development.

"Reacting to events is not good enough," says Harald Lochert. "The PTSS has to think ahead at all times and anticipate future needs. Staying one step ahead is the only way for us to be fast enough."

The programme may be over, but work is continuing on developing the components and preparing them for new challenges.

Two product teams introduce themselves.

Interview with Arie Band, Product Owner in the Forensic Fusion Team

Mr Band, how long have you been working at the PTSS? How would you describe your team?
I joined the PTSS in January 2020. We use the Scrum method, so all team members work together to develop the product. The team consists not only of software developers, but also of business analysts, testers, etc. We also have a Scrum master who handles coordination tasks.

What exactly is your role as product owner?
In Scrum, there are no team leaders in the traditional sense. I am part of the team, and my main task is to agree with everyone what we will do during our fortnightly cycles.

A key aspect of my role is maintaining and prioritising the product backlog to ensure that we are always focusing on the tasks that are currently essential. I also represent all stakeholders' interests – their requirements, needs and restric-

> "My main task is to agree with everyone what we will do during our fortnightly cycles."
>
> Arie Brand, Product Owner

tions – and ensure that the product remains aligned with our strategy over the long term. I am responsible for the product and its ongoing development, while the team is responsible for implementation.

Can you tell us about the specific products your team is responsible for?

Our team is responsible for four components. One of these is called ISS Viewer, and it was developed so that users can still access data from ISS now it has been shut down. The second component is WMC, which stands for Warrant Management Component. This is responsible for managing surveillance orders and synchronising them with the other components, such as ISS Viewer, FLICC and RDC. RDC, the Retained Data Component, enables users to access historical data. The fourth component is IRC, the Information Request Component. This enables information about telecommunications service subscribers to be shared between TSPs and law enforcement agencies. In other words, it's like a telephone directory.

What roles are there in your team?

We are quite a big team. As I mentioned earlier, all team members are referred to as developers, but they have different areas of expertise. For example, there are testing experts who create the testing strategy and ensure the quality of the content provided. Then there are the software developers, i. e. the people who code our software and make the necessary changes to the components. The architects help us to embed the software solution in the overall architecture. As already mentioned, the Scrum master handles coordination tasks, looks after the team and ensures compliance with the Scrum methodology. And finally there's me, the product owner.

Within the team, we have employees from a variety of international, professional and linguistic backgrounds. This diversity enables us to tackle all kinds of challenges.

Interview with Christoph Nickel, Product Owner in the Code Spotters Team

Mr Nickel, can you briefly introduce yourself and your team? Who are you and what do you do?

I have been working at the PTSS as product owner in the Code Spotters Team for a year. My team is in charge of developing the software for the FLICC backend. This is the part of the software that works in the background and is responsible for receiving and processing data. We chose the name Code Spotters because we are the people who look closely at the code and examine every bit and byte.

We consist of the team who developed this software, i. e. the PTSS Special Cases Team, and external contractors.

What is your team currently working on?

We are always working on improving the product. At the moment, we are also in the process of fixing some bugs that were brought to our attention by law enforcement agencies.

What is your biggest challenge at the moment?

In my team, it is probably prompt testing and all the automation that involves. It's a challenging but motivating task, as the complexity of the data tests our analytical skills, but also encourages creativity and team spirit in looking for innovative solutions.

What makes your team unique?

Many of our team members are specialists in telecommunications and have been working in this field for decades. In terms of expertise, we are very well covered. We have the skills we need for every technical and professional issue that may arise.

"The complexity of the data puts our analytical skills and creativity to the test."

Christoph Nickel, Product Owner

Training and advice

In-person courses are really appreciated

Telecommunications technology is constantly evolving and becoming more and more complex. As a result, using the PTSS processing system, and in particular interpreting the surveillance data, is an ongoing challenge and increasingly requires in-depth knowledge of the subject. Users of the system come from a wide range of backgrounds, and the PTSS offers training courses to ensure they all reach the same level. Janine Lüthi and Guillaume Pillonel tell us more.

As head of training at the PTSS, Janine Lüthi manages the service's portfolio of training courses for processing system users. Because participants range from experienced specialists to occasional users, it is essential to offer a selection of courses that can meet every individual's needs.

Ms Lüthi, can you tell us why the PTSS started offering its training courses?
The widespread shift to online communication has made interpreting surveillance data less straightforward. Technological developments have also led to an evolution of our legal frameworks. With this in mind, the PTSS began offering specific training courses. They have been developed over a number of years in response to demand from law enforcement authorities and in line with their needs.

Training for users and other stakeholders has been an explicit part of the PTSS's legal mandate since the new SPTA came into force in March 2018.

Demand for online training is growing all the time. Have the PTSS's training courses kept pace with this trend?
As you would expect, we have been keeping a close eye on this development. For example, our users can access training videos and step-by-step

Niklaus Hutmacher, Janine Lüthi and Guillaume Pillonel (from left to right) preparing for a training session

instructions for components such as IRC and WMC directly from their workstations. However, we also offer classroom-based courses, such as the basic course on mobile telephony. These generally last a full day. In some cases, they are supplemented by a second day of practical training, which enables participants to use the tools and software in near-real conditions. Because our users come from all over Switzerland, we give our courses in German, French and Italian, and sometimes in English. We also offer training days to familiarise users with the PTSS's work. These have been a great success.

"In 2024, over 500 people took part in around 40 training courses offered by us."

Janine Lüthi

How many training courses have you organised this year?

In 2024, over 500 people took part in the 40 or so training courses we provided. Most of the courses we offer are fully booked, and we often have to increase capacity to meet the ever-growing demand. Recently, I've seen a growing interest in tailor-made courses delivered directly to our customers.

What are the challenges you face as head of training?

Things that are relevant today may be irrelevant tomorrow, so we have to continue training our staff and keep our courses and documentation up to date. We have also noticed that expectations of our training are growing faster than our resources. We're delighted that our customers like what we are offering, but it's sometimes difficult to keep up with demand.

Guillaume Pillonel is head of the Incident Management Team. Most members of this team are also trainers. And for good reason: they know the components of the processing system inside out. As they intervene whenever technical problems occur during surveillance measures, they are familiar with all the scenarios that can arise in relation to the processing system and its components.

Mr Pillonel, in addition to providing training courses, your team is responsible for incident management. Can you tell us exactly what that involves?
Our role is to provide technical supervision and support for users of the PTSS processing system. We manage data transmission issues that arise during day-to-day operations, factoring in the urgency and importance of each situation. As such, we need to be able to react quickly, which often means we have to offer alternative solutions until the problem can be resolved permanently.

Collaboration with the other teams within the PTSS is essential. We often have to coordinate between the technical teams in-house and at the relevant TSPs. Our users are always our top priority.

And finally, one of my team's main tasks is ensuring that the various components of our processing system are running properly. This enables us to respond immediately if a problem arises.

Could you give us a concrete example of the assistance your team provides?
One example that springs to mind is emergency searches. If needed, we can draw on our experience to help users interpret the data they receive. As such, we can provide significant added value in complex emergency search scenarios. Our work helps to locate missing persons and potentially save lives.

What qualities do you expect your team members to have?
First of all, they need to be highly adaptable. The members of my team have to be able to run technical training courses for classes of 20 people, as well as being capable of handling urgent incidents. Stress management and quick thinking are essential qualities in critical situations. A pragmatic mindset and in-depth knowledge of new technologies are also vital.

> "Our work helps to locate missing persons and potentially save lives."
>
> Guillaume Pillonel

Mobile measurements

Audits to verify location data

In recent years, the PTSS, the Zurich Cantonal Police and the three mobile network operators (Swisscom, Sunrise and Salt) have carried out several joint audits. The aim of these was to verify the integrity and reliability of the data provided by entities that are obliged to cooperate. At the PTSS's request, the surveillance test drives required for the audits will be conducted regularly in future. An interview with Stefan Schär from the PTSS and René Odermatt from the Zurich Cantonal Police reveals more.

At the PTSS offices, there is a department with an impressive collection of mobile devices. The Compliance and Supervision Team is home to an inconspicuous grey metal cabinet containing a wide variety of smartphones, tablets and smartwatches – from older models to the latest Apple and Samsung devices. These are used to carry out tests to ensure that the surveillance measures deliver what they are supposed to: the right data. The PTSS conducted around 76 test surveillances in 2024 to identify any problems in advance.

Most of these tests take place on the PTSS's premises, however, which means they are limited in some ways.

For every internet or call connection, mobile phone providers log the location of the mobile phone masts involved in the communication. As required by law, the telecommunications service providers (TSPs) send this location information to the PTSS for surveillance purposes. When verifying the accuracy of the information, the Compliance and Supervision Team always uses

Stefan Schär from the Compliance & Supervision team evaluates the measured test location data.

The surveillance measures should deliver what they are supposed to deliver: the right data.

the same mobile phone mast as the reference point for stationary tests. This approach works well when checking the format of the data that is sent. However, it will not detect any inconsistencies relating to mobile surveillance targets.

But now let's take a look at the canton of Zurich, where a cantonal police car is driving through a rural area in the lowlands. Behind the driver are mobile communication measuring devices, laptops, screens full of technical code, maps and time displays. The cantonal police officers run through several scenarios: calls, streaming, messenger services and web browsing. They drive systematically through cities and towns, as well as through rural areas with poor or no reception. All of this is designed to help verify location detection during surveillance. The PTSS has shared the test scenarios it uses for these test trips and, working with the Zurich Cantonal Police, has determined additional test options to be used in a mobile environment. The Zurich Cantonal Police provides its expertise and the measuring systems required for the full audit, while the PTSS coordinates the tests with the TSPs.

The Zurich Cantonal Police will continue to carry out this audit periodically in the future, in close cooperation with the PTSS. Stefan Schär from the PTSS's Compliance and Supervision Team and René Odermatt, Mobile Forensics Expert at the Zurich Cantonal Police, explain all in this interview.

During test drives, various parameters are measured at short intervals.

Interview with René Odermatt and Stefan Schär

What is your background and what are your duties at the PTSS/the cantonal police?

Schär: Shortly after finishing my apprenticeship, I specialised in telecommunications systems. Later, I completed two master's degrees in IT and digital forensics. As a compliance specialist at the PTSS, I am responsible for ensuring the integrity and completeness of the data in our surveillance system (telecommunications surveillance processing system). I'm quite a fastidious person, and I can put that quality to good use here!

Odermatt: I worked in the mobile network planning and optimisation private sector for 15 years, and I have now been an expert in mobile forensics at the Zurich Cantonal Police for over ten years. We use scientific methods to analyse communication data from mobile networks. Our daily work includes answering questions such as whether a mobile phone was at a specific location.

How did this collaboration come about?

Schär: Our collaboration emerged almost naturally. The PTSS operates the telecommunications surveillance processing system and manages the test devices. The Zurich Cantonal Police has the equipment we need to complement our own. We are also in close contact with TSPs in our daily work, so we act as a crucial link between them and the police.

Odermatt: Exactly. We've been helping with mobile phone tracking throughout Switzerland for ten years. For example, we assist with missing person searches. The equipment needed for this, such as the measuring systems used in our audits, requires a significant investment – not only financially, but also in terms of acquiring expertise.

Our reports are based on historical surveillance data. This means that the data from the test trips is particularly valuable because it supplements the historical data.

> "Our daily work includes answering questions such as whether a mobile phone was at a specific location."
>
> René Odermatt, Zurich Cantonal Police

"The aim of the tests is to verify and guarantee the integrity of the secondary data supplied by the TSPs."

Stefan Schär, PTSS

Can you briefly explain how your latest test trips went?

Schär: I was responsible for central coordination of the work between the Zurich Cantonal Police, the TSPs and the PTSS. This included distributing information and preparing the upcoming audits, activating surveillance of the test devices, using raw data to analyse the problems we identified, and coordinating follow-up tests and checks to verify that the TSPs had rectified errors. We worked with the Zurich Cantonal Police to determine the test scenarios in advance.

Odermatt: We worked with the PTSS to design these scenarios and plan the surveillance test trips in a way that reflects participants' normal mobile communication behaviour. This means travelling through urban and rural areas, including places with poor network coverage. We processed and verified the data supplied by the TSPs, comparing the time stamps and reported location information with the data collected during the test trips. We then forwarded any inconsistencies we identified to the PTSS for further investigation.

Schär: Problems or inconsistencies were reported to the TSPs as soon as they were identified. I should mention that our cooperation with the TSPs was good, too. They rectified all the problems we reported to them very quickly.

What is the purpose of these tests? Can't they be run by the mobile network operators?

Schär: The aim of the tests is to verify and guarantee the integrity of the secondary data supplied by the TSPs. We focus in particular on the location data, which we compare with the recorded data from the vehicle. If we discover any discrepancies, they have to be analysed in detail.

Centralised coordination and implementation is the only way to ensure that the tests are carried out uniformly and consistently. Every TSP would probably organise its tests in a slightly different way, so the results would not be fully comparable.

Odermatt: And apart from that, it takes a lot of expertise to identify the call scenarios in the data. In order to share our findings, we sent the final report to all law enforcement agencies.

"We planed the test trips in a way that reflects participants' normal mobile communication behaviour."

René Odermatt, Zurich Cantonal Police

What challenges do you think surveillance will face in the future? In relation to technology, for instance?

Odermatt: I think growing complexity is the biggest challenge. This can be overcome by close cooperation between the stakeholders involved, such as TSPs, the PTSS and law enforcement authorities.

Schär: There are a number of technical challenges associated with 5G, such as the significantly higher data rates that have to be processed and the concealment of subscriber identities by using temporary identifiers.

What did you particularly enjoy about the collaboration?

Schär: Our work together was friendly and cooperative. The main thing I appreciated was how quickly everyone responded to each other, including the TSPs.

Odermatt: Everybody communicated openly, and we had the support we needed at every level. During the debriefing, things that had not gone as well as they could have were discussed head-on and will be taken into account in the next audit. We all had the same goal in mind, and we were able to build on our experience from previous audits. As we've already mentioned, none of this can be achieved unless TSPs, the PTSS and law enforcement agencies work together.

03

FACTS AND FIGURES

Reasons for surveillance

In 2024, Swiss law enforcement agencies and the Federal Intelligence Service (FIS) ordered more than twice as many surveillance measures from the PTSS.

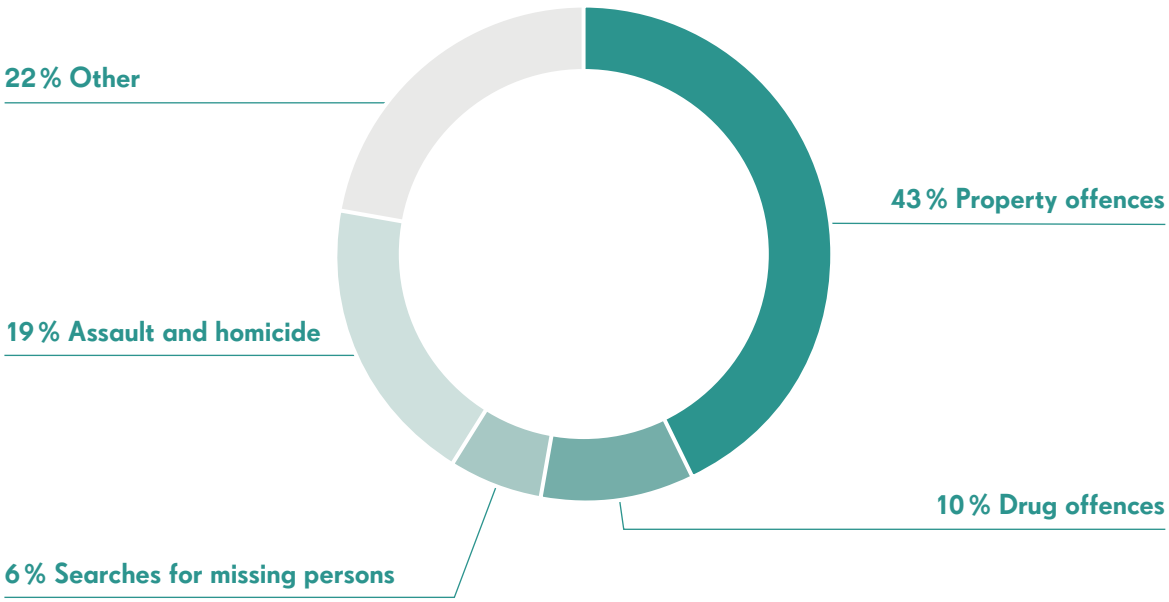
The sharp increase in surveillance measures is mainly due to the significant rise in antenna searches. For the first time in years, the number of antenna searches has doubled compared with the previous year.

Real-time surveillance measures have also increased by around 45 per cent. The number of retroactive surveillance operations is around a quarter higher than last year. Emergency searches have risen by a fifth. Only the number of searches is slightly below last year's level.

There has also been an increase in the number of requests for information. In 2024, the PTSS provided around 20 per cent more information (both simple and complex).

In 2024, 43 per cent of all surveillance measures related to property offences. The number of measures related to property offences more than tripled compared to the previous year. Orders based on criminal offences against life and limb also more than doubled. 10 per cent of measures were carried out to investigate serious violations of the Narcotics Act.

You can find further information on our statistics at: **www.li.admin.ch/en/stats**



Definition and number of surveillance measures and types of information

Real-time surveillance (1)
Real-time surveillance is the simultaneous, slightly delayed or repeated transmission of post or telecommunications data to the law enforcement services over the processing system.

Retroactive surveillance (2)
Retroactive surveillance includes data on who has been in contact with whom, when, how, for how long and from where, for a maximum period of six months in the past.

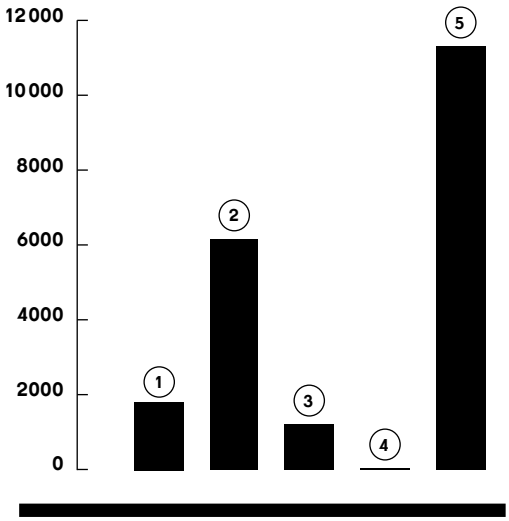
Searches for missing persons (3)
The purpose of these searches is to locate and rescue people, such as injured hikers or missing children.

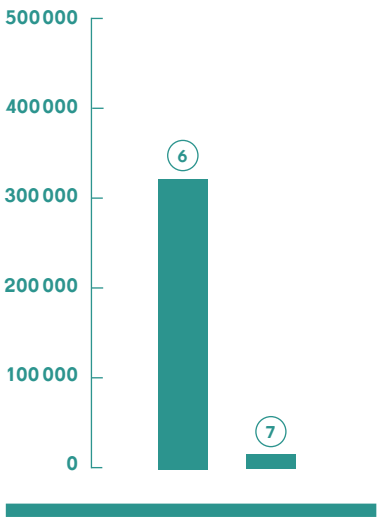
Searches for convicted persons (4)
A criminal search enables law enforcement services to locate the whereabouts of people on whom a custodial sentence has been imposed or against whom a measure involving deprivation of liberty has been ordered in a legally binding and enforceable judgment.

Antenna search (5)
An antenna search includes the retroactive surveillance of all communications, communication attempts and network accesses that have taken place at a specific location via specific mobile radio cells or a specific public WLAN access during a given period of time.

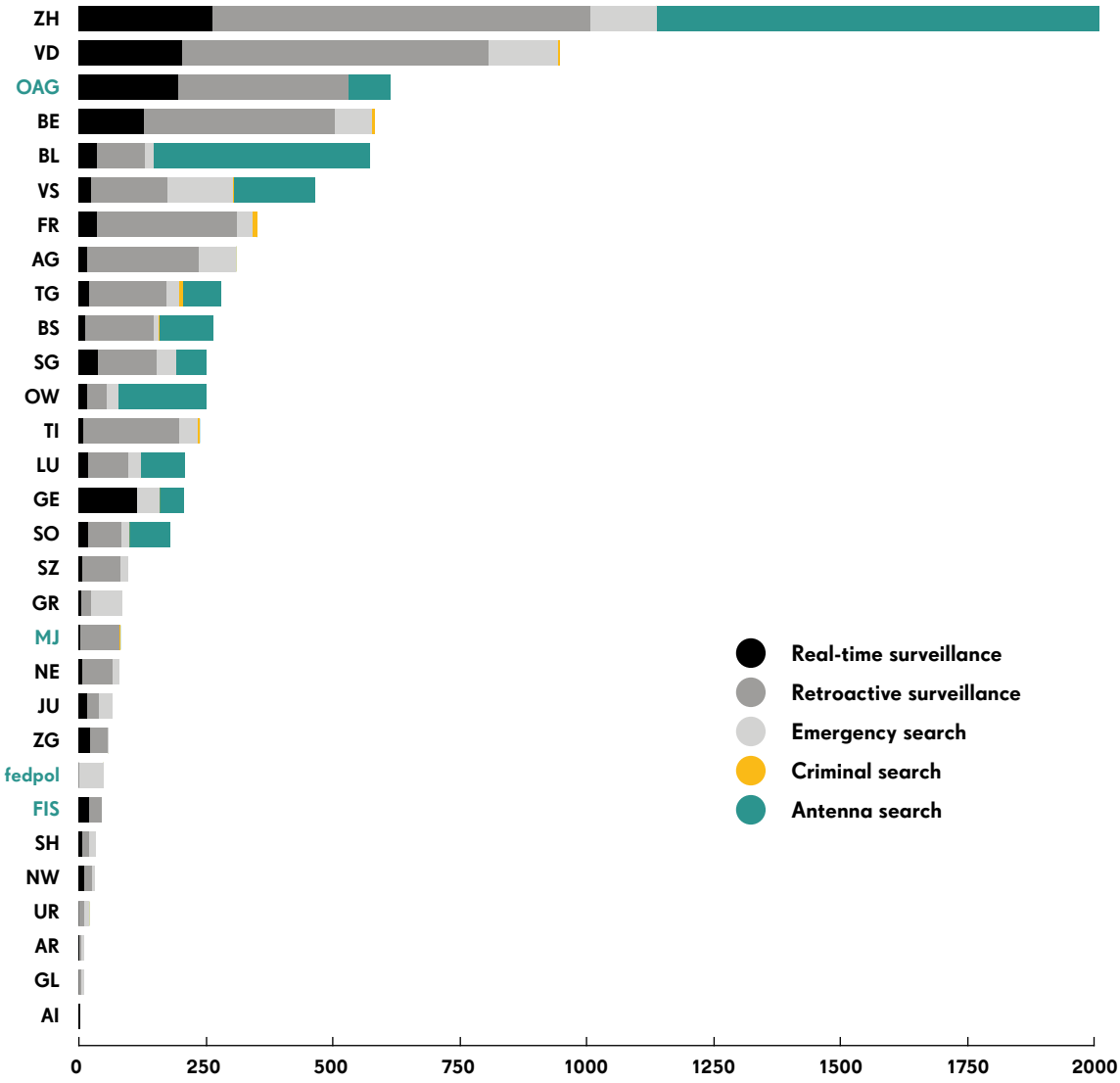
Simple information (6)
Simple information includes basic information on telecommunication connections, for example who the subscriber of a particular telephone number or IP address is.

Complex information (7)
Complex information provides more detailed information on telecommunications connections, including copies of contracts and identity documents.





Mandates from the federal government and cantons

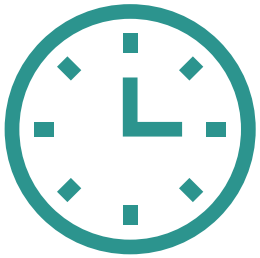


OAG Office of the Attorney General
MJ Military Justice
FIS Federal Intelligence Service
fedpol Federal Office of Police

Number of enquiries from the public

22

Number of on-call assignments



2080

Registered users processing system

WMC 4283
Warrant Management Component

IRC 6183
Information Request Component

RDC 2845
Retained Data Component

FLICC 2806
Federal Lawful Interception Core Component (real-time)

Number of Special Cases

144

(See p. 9, Provider Management, Special Cases Team)

PTSS financial performance in CH

Total revenue
25 m

Total expenditure
46.7 m

Federal contribution
21.7 m

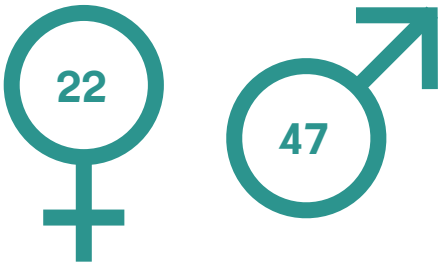
Number of media enquiries

5

Number of employees

69

Numbers of women / men



Average age

47.8

First language

63 % German

3.6 % Italian

31.5 % French

1.9 % Other

Age distribution

20 to 29
2.9 %

30 to 39
23.2 %

40 to 49
20.3 %

50 to 59
46.4 %

60 to 69
7.2 %

“Staying one step ahead is the only way for us to be fast enough.”

Harald Lochert, head of the Systems Team (Provider Management)

Impressum

Editing: PTSS
Realisation: Schön & Berger, Zurich
Printing: Druckerei Ruch, Ittigen
Photos: Cover shutterstock,
p. 4 id-k Kommunikationsdesign AG (project, postproduction), Silvia Rohrbach (photo)
p. 8 Media und Event Services (MS-AMC-MES) FOITT
p. 18, 19, 21, 23, 25 mk-photography (Miriam Kolmann)
p. 26 Kapo ZH
Illustrations: p. 27/28 Bianca Litscher, Lucerne
Font: Minion Pro, Drescher Grotesk
Paper: Z-Offset
Language: German, French, Italian and English

■

In the interests of legibility and comprehension, we have refrained from using complex technical and legal terms. We have also tried to use gender-neutral language wherepossible.

Federal Department of Justice and Police FDJP
Post and Telecommunications Surveillance Service PTSS
3003 Bern